Research Paper | Engineering | E-ISSN No : 2454-9916 | Volume : 3 | Issue : 10 | Oct 2017

# SECURE DATA SHARING BY ENCRYPTION OF IDENTITY BASE WITH REVOCABLE STORAGE

Rutambh Trivedi [1] | Shyamsundar Kosbatwar [2]

[1] Department of Computer Engineering, SKN Sinhgad College of Engineering, Pune, India - 411041.
[2] Professor, Department of Computer Engineering, SKN Sinhgad College of Engineering, Pune, India - 411041.

## ABSTRACT

A Cloud computing is really a feasible way for sharing the data and its fast and reliable. It can be beneficial for both society and the users who are using that. But sometime it happens that user upload the data to the cloud server and it contains the very valuable information or private information. That's why it is necessary to keep the track of the data and secure that by crypto graphically,

Identity based encryption can be useful for develop the crypto graphical tool for this issue. Thus we cannot ensure that its will be static. Main issue is that the when the certain user's authorization will expire than it should be removed from the Process, and also ensure that the user who is revoked cannot access the data that is previously shared. For maintaining this issue we are developing the recoverable storage identity based Encryption RSIBE, with giving cipher text and security of forward and back end user. In this user revocation will also include. The security model will also developed. When we compared our RSIBE it can be beneficial for the users in the areas of performance, functionality and efficiency and it can also be low in the cost. And then at the end we will provide the implementation results for comparing.

**KEY WORDS:** Cloud computing, Revocation, Cipher text, Security, Identity Based, Data Sharing.

## INTRODUCTION:

Cloud Computing is feasible for the give the huge amount of complex computing and the benefits to the user and the in cloud computing the user can access his/her data at any platform and anytime and anywhere for example mobile devices and personal computers that's why it's really convenience way for the users. There are many cloud available this time for example Apple's, Microsoft's, Amazon's S3.But the primary concern for this is the issue of the security in the cloud.

First of all when user upload the data to the cloud it's no longer in his/her hands so user can't control the data and that's why user don't think that's its secured. The second concern is that the cloud is the open environment so the number of attacks will be huge. That's why it's necessary to give authorization to the users that when the authorization expires they can't access the data. That's why users wants to share the data only with those who had the authorization and cannot use the valuable information or misuse that. Main problem is the use the access of identity base encryption for the given system.

## MATERIALS AND METHODS:

### Technologies Used:

During the solution development, following hard-wares were used:

- 250 GB HD
- 4GB RAM
- Cloud Environment
- Wireless Router

### Software Requirement:

- ASP.NET
- Cloud Environment

### Results:

**Table 1: Comparison of Communication and Previous work**

| Schemes | Private key size | Update key size | Ciphertext size |
|---|---|---|---|
| Libert and Vergnaud | O(log N )$\tau_{G1}$ | O(r log N/r)$\tau_{G1}$ | O(1)τG1 + O(1)τG2 |
| Seo and Emura | O(log N )$\tau_{G1}$ | O(r log N/r)$\tau_{G1}$ | O(1)τG1 + O(1)τG2 |
| Liang et al. | O(1)$\tau_{G1}$ | O(1)$\tau_{G1}$ | O(1)τG1 + O(1)τG2 |
| Our scheme | O(log N )τG1 | O(r log N/r)τG 1 ‡ | O(log(T )2)τG1 + O(1)τG2 |

**Table 2: Comparison of Complexity with Previous Works**

| Schemes | Encryption | Decryption | CT Update |
|---|---|---|---|
| Libert and Vergnaud | O(1)$e$ + O(1)$p$ | O(1)$p$ | 0 |
| Seo and Emura | O(1)$e$ + O(1)$p$ | O(1)$p$ | 0 |
| Liang et al. | O(1)$e$ + O(1)$p$ | O(1)$p$ | (O(N ))$e$ + O(1)$p$ |
| Our scheme | O(log T )$e$ + O(1)$p$ | O(1)$p$ | O(log(T )$^2$)$e$ + O(1)$p$ |

**Table 3: Comparison of Security and Functionality with Previous Works**

| Schemes | Model | Assumption | PKU | PCU | CA | DKE | FS | BS |
|---|---|---|---|---|---|---|---|---|
| Libert and Vergnaud | Adaptive | DBDH | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ |
| Seo and Emura | Adaptive | DBDH | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ |
| Liang et al. | Adaptive | DBDH | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ |
| Our scheme | Adaptive | ℓ-dBDHE | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

## PROPOSED METHODOLOGY

Cipher text extension introduced by this paper, the number of cipher text to shared data available is same as the number of share data updated. Proxy re-encryption can be useful for terminate the problem of efficiency. But that requires the user to interact with cloud so that shared data can be converted to Cipher text.

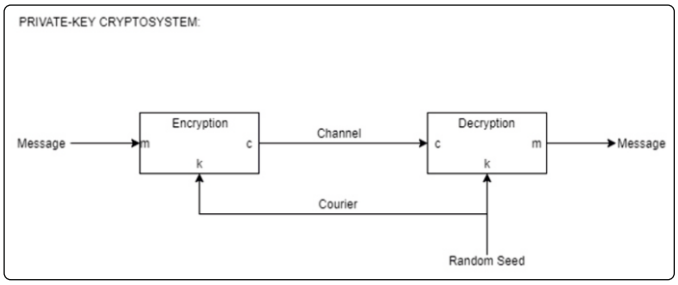


**Fig.1: Private key Cryptosystem**

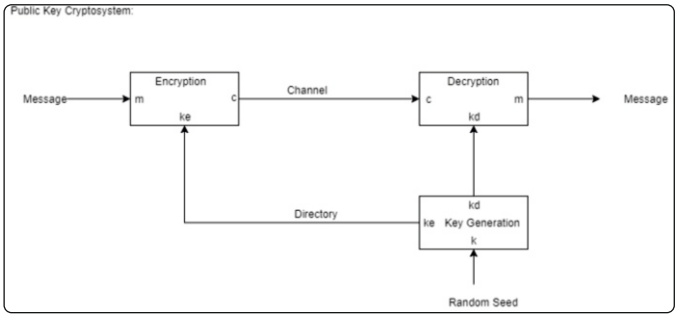


**Fig 2: Public key Cryptosystem**

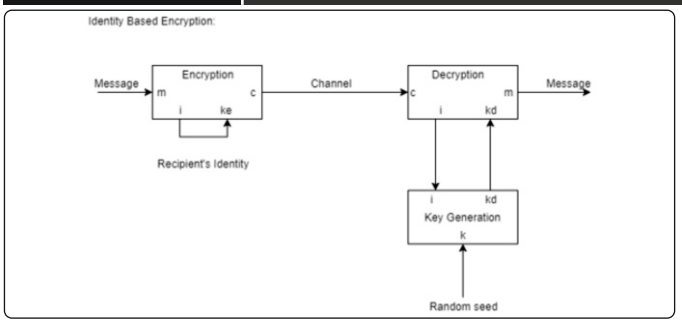


**Fig.3: Identity based Encryption**

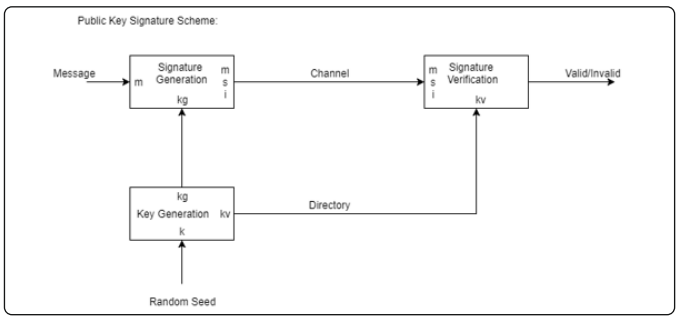


**Fig.4: Public Key Signature Scheme**

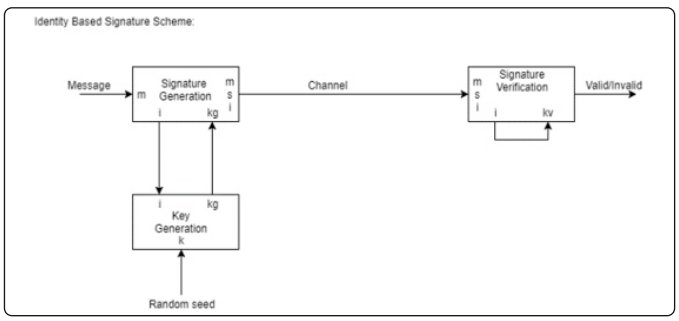


**Fig.5: Identity Based Signature Scheme**

**CONCLUSION:**

Cloud computing is good for users so that they can access the data anywhere anytime. In this paper, we are building cost effective and secure data sharing system, we proposed a notion called RS-IBE, which can be useful for identity revocation and cipher text update simultaneously so that way revoked user can be prevented from accessing previously shared data, as well as subsequently shared data. The RS-IBE scheme is better for security in the standard model, under the decisional ℓ-DBHE assumption. The results shows that our scheme has advantages in terms of efficiency and functionality, and it's more reliable in practical applications.

**REFERENCES:**


1. L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.
2. K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," Services Computing, IEEE Transactions on, vol. 5, no. 4, pp. 551–563, 2012.
3. C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.
4. G. Anthes, "Security in the cloud," Communications of the ACM, vol. 53, no. 11, pp. 16–18, 2010.
5. K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.
6. B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in INFOCOM, 2013 Proceedings IEEE. IEEE, 2013, pp. 2904–2912.
7. S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384–394, 2014.
8. C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 468–477, 2014.
9. A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in cryptology. Springer, 1985, pp. 47–53.
10. D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586– 615, 2003.
11. W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology–CRYPTO 1998. Springer, 1998, pp. 137–152.
12. D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in Advances in Cryptology– CRYPTO 2001. Springer, 2001, pp. 41–62.
13. C. Gentry, "Certificate-based encryption and the certificate revocation problem," in Advances in Cryptology–EUROCRYPT 2003. Springer, 2003, pp. 272–293.
14. V. Goyal, "Certificate revocation using fine grained certificate space partitioning," in Financial Cryptography and Data Security. Springer, 2007, pp. 247–259.
15. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proceedings of the 15th ACM conference on Computer and communications security. ACM, 2008, pp. 417–426.
16. B. Libert and D. Vergnaud, "Adaptive-id secure revocable identity-based encryption," in Topics in Cryptology–CT-RSA 2009. Springer, 2009, pp. 1–15.
17. ——, "Towards black-box accountable authority ibe with short cipher texts and private keys," in Public Key Cryptography–PKC 2009. Springer, 2009, pp. 235–255.
18. J. Chen, H. W. Lim, S. Ling, H. Wang, and K. Nguyen, "Revocable identity-based encryption from lattices," in Information Security and Privacy. Springer, 2012, pp. 390–403.
19. J. H. Seo and K. Emura, "Revocable identity-based encryption revisited: Security model and construction," in Public-Key Cryptography–PKC 2013. Springer, 2013, pp. 216–234.
20. ——, "Efficient delegation of key generation and revocation functionalities in identity-based encryption," in Topics in Cryptology– CT-RSA 2013. Springer, 2013, pp. 343–358.
21. K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing," in Computer Security-ESORICS 2014. Springer, 2014, pp. 257–272.
22. D.-H. Phan, D. Pointcheval, S. F. Shahandashti, and M. Strefler, "Adaptive cca broadcast encryption with constant-size secret keys and cipher texts," International journal of information security, vol. 12, no. 4, pp. 251–265, 2013.
23. M. Bellare and S. K. Miner, "A forward-secure digital signature scheme," in Advances in Cryptology–CRYPTO 1999. Springer, 1999, pp. 431–448.
24. M. Abdalla and L. Reyzin, "A new forward-secure digital sig-nature scheme," in Advances in Cryptology–ASIACRYPT 2000. Springer, 2000, pp. 116–129.
25. A. Kozlov and L. Reyzin, "Forward-secure signatures with fast key update," in Security in communication Networks. Springer, 2003, pp. 241–256.
26. X. Boyen, H. Shacham, E. Shen, and B. Waters, "Forward-secure signatures with untrusted update," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006,pp. 191–200.
27. J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen, "Forward-secure identity-based signature: security notions and construction," Information Sciences, vol. 181, no. 3, pp. 648–660, 2011.
28. R. Canetti, S. Halevi, and J. Katz, "A forward-secure public-key encryption scheme," in Advances in Cryptology–Eurocrypt 2003. Springer, 2003, pp. 255–271.
29. D. Yao, N. Fazio, Y. Dodis, and A. Lysyanskaya, "Id-based encryption for complex hierarchies with applications to forward security and broadcast encryption," in Proceedings of the 11th ACM conference on Computer and communications security. ACM, 2004, pp.354–363.
30. J. M. G. Nieto, M. Manulis, and D. Sun, "Forward-secure hierarchical predicate encryption," in Pairing-Based Cryptography–Pairing 2012. Springer, 2013, pp. 83–101.
31. A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and cipher text delegation for attribute-based encryption," in Advances in Cryptology–CRYPTO 2012. Springer, 2012, pp. 199–217.
32. B. Waters, "Efficient identity-based encryption without random oracles," in Advances in Cryptology–EUROCRYPT 2005. Springer, 2005, pp. 114–127.

**Books:**

1. S. Micali, "Efficient certificate revocation," Tech. Rep., 1996.
2. B. Lynn. (2014) Pbc library: The pairing-based cryptography library.

**Proceedings Papers:**

1. X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "Cost-effective authentic and anonymous data sharing with forward security," Computers, IEEE Transactions on, 2014, doi: 10.1109/TC.2014.2315619.